BrisDoc Patient care by people who care

NHS

Data Breach Notification Procedure

Version:	Owner:	Created:
1.3	Dr Kathy Ryan (Medical Director)	1st February 2022
Published:	**Approving Director:**	**Next Review**
04/08/2025	Rhys Hancock (Director of Nursing, AHPs and Governance.)	04/08/2026

Contents

Introduction

BrisDoc is committed to protecting the personal data of all individuals we work with, including patients, staff, and partners. Despite robust controls, there may be occasions where a data breach occurs.

This procedure sets out how to identify, report, assess, and respond to personal data breaches. Prompt action helps to minimise harm, meet our legal obligations under UK GDPR and the Data Protection Act 2018, and maintain trust in our services.

A data breach refers to any incident where personal data is accidentally or unlawfully:

- Lost or destroyed
- Disclosed to someone without authorisation
- Altered without permission
- Accessed by unauthorised individuals
- Examples of incidents that must be reported include:
- Loss or theft of personal data (e.g. paper files, laptops, USBs)
- Sending personal data to the wrong recipient
- Unauthorised sharing or access to personal information
- Corruption or unauthorised changes to personal records

All suspected or actual breaches must be reported immediately – or as soon as possible – to the Caldicott Guardian and/or Information Governance (IG) Lead.

Once notified, the following actions will take place:

- The Board of Directors and Data Protection Officer (DPO) will be informed.
- The breach will be assessed to determine its severity and potential impact on individuals.
- A decision will be made on whether the affected individuals and the Information Commissioner's Office (ICO) need to be notified.
- If required, affected individuals will be informed without delay.
- All decisions and actions will be recorded in the Data Breach Register.

We have a legal duty to report certain breaches to the ICO within 72 hours of becoming aware of them. Therefore, it is essential that all staff act promptly and always follow this procedure, including weekends and bank holidays.

Reporting a Breach

All staff have a responsibility to report any actual or suspected data breach as soon as they become aware of it.

A data breach could include:

- Sending personal or patient data to the wrong person
- Losing a paper file, laptop, containing personal or patient information
- Unauthorised access to digital records
- Accidentally sharing information with someone who shouldn't have it

What to do if you identify or are informed about a potential breach:

1. Log a Learning Event
   Report the issue on the BrisDoc Learning Event portal without delay. Include all relevant information such as what happened, when, and who was involved.
2. Notify the Governance Team
   The Governance team must inform the Senior Information Risk Officer (SIRO) and/or Caldicott Guardian (or their Deputy) by email within 24 hours of receiving the report.
3. Initial Assessment
   The SIRO and/or Caldicott Guardian will review the details to determine whether a data breach has occurred and assess how serious it is.
4. Investigation and Escalation
   If the breach is confirmed, further investigation will begin. The Data Protection Officer (DPO) and Board of Directors will be informed where necessary.
5. Timelines Matter
   Some breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of being identified. This deadline includes weekends and bank holidays, so it is essential that concerns are reported immediately.
6. Ongoing Communication
   Staff may be contacted for more information as part of the investigation. Updates and outcomes will be shared where appropriate.

Reporting promptly helps protect individuals' data, limits any harm, and ensures BrisDoc meets its legal responsibilities.

If you're ever unsure whether something is a breach, report it – it's better to raise it and have it reviewed than risk missing something important.

Appendix 1 - Breach Assessment Reporting and Management Process

Identifying and Reporting a Breach

- A potential or actual data breach is identified (e.g. through audit, observation, or system alert, Connecting Care Family Audit, CLEO/ADASTRA – EMIS Audit).
- The staff member who identifies or is informed about the breach must:
    - Log a Learning Event on the BrisDoc portal as soon as possible.
    - Provide relevant details such as when the incident occurred and what data may be involved.

Initial Notification

- The Governance Team must:
    - Notify the Information Governance (IG) Lead and Caldicott Guardian (CG)/Deputy by email within 24 hours.
    - Include the Learning Event reference and a summary of the incident.

Assessment and Triage

- The SIRO and/or CG will:
    - Assess whether the incident qualifies as a personal data breach.
    - Evaluate the severity using the Breach Assessment Grid (see Appendix 2).
    - Confirm whether BrisDoc is the Data Controller for the data involved.
    - Report a summary of the assessment at the next IG Board meeting.

Notification to DPO and ICO (if required)

- If the breach is deemed reportable:
    - The DPO is informed.
    - The breach is submitted via the Data Security and Protection Toolkit (DSPT) within 72 hours.
    - The DSPT tool automatically notifies the Information Commissioner's Office (ICO).

- The DPO liaises with the ICO and provides updates to relevant stakeholders (IG Lead, CG, etc.).

Investigation

- Internal investigations begin:
  - A staff investigation and/or IG investigation is initiated.
  - An Action Plan is created (led by People Team, IG, or both as needed).
  - A Final Report is written, shared with relevant parties, and added to the incident log.
  - A summary is provided to the next IG Board.

Where BrisDoc is *not* the Data Controller

- The appropriate Data Controller is informed immediately to enable reporting within 72 hours.
- BrisDoc will:
  - Support any investigation or action required.
  - Assist with communication to affected individuals or enforcement authorities if needed.

Learning and Continuous Improvement

- Outcomes from the investigation are used to:
  - Update relevant processes and documentation.
  - Feed into training and awareness materials.
  - Reduce the risk of similar incidents in the future.

Appendix 2 – IG/Data Security Breach Assessment Grid

Impact Level

Low (1)	Minimal personal data, unlikely to cause harm or distress
Moderate (2)	Some personal or identifiable data; could cause minor inconvenience
High (3)	Special category data or moderate risk of harm/distress
Very High (4)	Sensitive data (e.g. health, criminal, safeguarding); likely to cause harm
Critical (5)	High-risk data exposure (e.g. children, large numbers, media interest)

Likelihood Score – How Likely Is It That Harm Could Occur?

Rare (1)	Unlikely the data will be accessed or misused
Unlikely (2)	Possible, but not expected to cause harm
Possible (3)	A realistic chance harm could occur
Likely (4)	Likely harm will occur without intervention
Almost Certain (5)	Harm is very likely or already occurring

Total Risk Score (Impact x Likelihood)

1–5	Low	Log locally. No ICO notification. Monitor for patterns.
6–10	Medium	Consider ICO notification if personal impact is unclear.
11–15	High	Likely ICO reportable. Notify DPO and assess mitigation actions.
16–25	Critical	Immediate action. Notify ICO and affected individuals without delay.

Appendix 3- DPO Data Breach Notification Procedure

If you believe a data breach may have occurred — or are unsure and need advice — contact the Data Protection Officer (DPO) as soon as possible. This is especially important because some breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours, including weekends and bank holidays.

Steps to Follow

1. **Notify the DPO Immediately**
    - Email**: dpo@brisdoc.org**
    - Do not delay reporting. Even if not all details are available yet, initial notification is important.
2. **Take Steps to Contain the Breach**
    - Try to recover the data or prevent further loss (e.g. ask the unintended recipient to delete the information securely).
    - Do not attempt to delete or alter records unless directed by the IG Lead or DPO.
3. **Send the Following Information to the DPO**
   Include as much detail as possible:
    - **Date of the breach**
    - **Date you became aware** of the breach
    - **Summary** of what happened
    - **Type of data involved** (e.g. name, address, health information)
    - **Number of people affected** (or an estimate)
    - Whether the **individual(s) are aware** of the breach
    - Whether any **other organisation is involved or aware**
    - Any **actions already taken** to reduce the impact
4. **Redact Personal Details Where Possible**

- If sending supporting documents, remove or black out personal identifiers unless the DPO specifically requests otherwise.

Why It's Important

Quick and clear reporting allows BrisDoc to:

- Meet legal requirements under UK GDPR
- Reduce harm to individuals
- Take appropriate actions with the ICO, if needed
- Learn from the incident and prevent future breaches

If you are ever unsure, it's always better to **report a potential breach** than to risk not reporting one at all.

Appendix 4 – Personal Data definition

What is a Personal Data Breach?

A personal data breach is any security incident that leads to:

- The accidental or unlawful destruction, loss, alteration, disclosure of, or access to personal data—whether that data is stored physically or digitally.

Breaches don't just mean data being "hacked" or stolen. They can include:

- Sending personal information to the wrong person
- Losing a paper file or device containing personal data
- Unauthorised people accessing records
- Accidentally changing or deleting personal information

A breach is assessed based on the risk to the rights and freedoms of the individual, not just whether the data was lost.

What is Personal Data?

Personal data is any information that can be used to identify a living person, either on its own or when combined with other information.

Examples include:

- Names, addresses, phone numbers, and email addresses
- NHS numbers or staff ID numbers
- Location data, online identifiers (like IP addresses), and device IDs
- Anything that links to someone's identity

What is Special Category Data?

Some types of personal data are considered especially sensitive and require more protection under the law. These are known as special category data and include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs

- Genetic data
- Health data
- Sex life or sexual orientation

Other Sensitive Categories (for BrisDoc Context)

In the context of BrisDoc services, the following are also treated as highly sensitive:

- Information about vulnerable children or adults
- Criminal convictions or prison records
- Mental health, sexual health, or communicable disease status
- Any data that could cause discrimination under the Equality Act 2010
- Any information likely to cause harm or distress if disclosed

Change Register

Date	Version	Author	Change Details
Feb-22	1.0	D Lowndes / DPO	After DPO review of all policies new procedure as drafted by DPO. Additional material because of recent incident
Mar-22	1.1	D Lowndes	Additional appendices added
July 2024	1.2	K Ryan	Removed names, changed incident to learning event and Appendix 1 changed wording.
June 2025	1.3	D Lowndes	Review and change of SIRO. Added CLEO.